

# Andrew Shallue

Curriculum Vitae – February 2016

## CONTACT INFORMATION

---

Department of Mathematics  
Illinois Wesleyan University  
1312 Park St Bloomington, IL 61701 USA

309-556-3587 (office phone)  
ashallue@iwu.edu

## PERSONAL INFORMATION

---

Citizenship: USA

Hobbies: soccer, medieval re-creation, strategy board games

## EDUCATION

---

- Ph.D. in Mathematics, University of Wisconsin–Madison, Summer 2007  
Subject: Algorithmic number theory  
Advisor: Eric Bach  
Minor: Computer Science
- B.A. in Mathematics (Summa Cum Laude), Gustavus Adolphus College, Spring 2000

## ACADEMIC POSITIONS

---

- Associate Professor of Mathematics, Illinois Wesleyan University, August 2015 - present
- Assistant Professor of Mathematics, Illinois Wesleyan University, August 2009 - August 2015
- Postdoctoral position, University of Calgary, August 2007 - July 2009  
Supervisor: Mark Bauer

## RESEARCH INTERESTS

---

Algorithmic and computational number theory; cryptography

## RESEARCH AGENDA

---

To be an expert on algorithmic problems related to pseudoprimes, including construction of rare pseudoprimes and tabulation of common ones. A particularly fruitful means for constructing pseudoprimes relies on solving a subset-sum problem, and so I plan to continue research in this area. However, my goal is to pursue breadth of knowledge rather than depth, and I anticipate working on other problems that catch my interest.

## PEER-REVIEWED PUBLICATIONS

---

- Eric Bach and Andrew Shallue. *Counting composites with two strong liars*. Accepted for publication by Mathematics of Computation. Submitted July 2013.
- W.R. Alford, Jon Grantham, Steven Hayman, and Andrew Shallue. *Constructing Carmichael*

*numbers through improved subset-product algorithms*, Mathematics of Computation, volume 83, number 286, 2014, pages 899–915.

- Andrew Shallue. *An improved multi-set algorithm for the dense subset sum problem*. In ANTS VIII; Algorithmic Number Theory Symposium (Banff, Canada). Lecture Notes in Computer Science 5011, Springer, Berlin, 2008.
- Andrew Shallue and Christiaan E. van de Woestijne. *Construction of rational points on elliptic curves over finite fields*. In ANTS VII: Algorithmic Number Theory Symposium (Berlin, Germany). Lecture Notes in Computer Science 4076, Springer, Berlin, 2006.

#### PUBLICATIONS UNDER REVIEW

---

- Andrew Shallue. *Tabulating pseudoprimes and tabulating liars*. Submitted for publication to ACM Transactions on Algorithms, August 2014.

#### NON PEER-REVIEWED PUBLICATIONS AND POSTERS

---

- *Tabulating pseudoprimes and tabulating liars*, a contributed poster in the poster session at ANTS XI; Algorithmic Number Theory Symposium (Gyeongju, Korea), 2014. See <https://ants2014.kookmin.ac.kr/accepted-posters.html>
- *Lifting Automorphisms of Quotients by Central Subgroups*, with Ben Kane, hosted at the arXiv.org e-print archive, submitted April 2013. See <http://arxiv.org/abs/1304.4632>
- *Constructing a ten billion factor Carmichael number*, a contributed poster in the poster session at ANTS X; Algorithmic Number Theory Symposium (San Diego, USA), 2012, with Steven Hayman. See <http://math.ucsd.edu/~kedlaya/ants10/accepted-posters.html>
- *Division algorithms for the fixed weight subset sum problem*, hosted at the arXiv.org e-print archive, submitted January 2012. See <http://arxiv.org/abs/1201.2739>
- *Faster construction of Carmichael numbers and other pseudoprimes*, a contributed poster in the poster session at ANTS IX; Algorithmic Number Theory Symposium (Nancy, France), 2010. See <http://ants9.org/acceptedposters.html>

#### SELECTED RESEARCH TALKS SINCE FALL 2009

---

- “Constructing large numbers with cheap computers;” invited talk for Butler Math Colloquium, September 2015
- “Constructing large numbers with cheap computers;” invited talk for Illinois College Colloquium, September 2014
- “Tabulating liars and witnesses;” contributed talk at Illinois Number Theory Day at UIUC, June 2014

- “Constructing a 10 billion factor Carmichael number;”  
invited talk for a special session at the Canadian Math Society Summer Meeting, June 2013
- “Constructing a 10 billion factor Carmichael number;”  
invited talk for a special session at the Joint Mathematics Meetings, January 2013
- “Constructing large numbers with cheap computers;”  
invited talk for IWU faculty colloquium, September 2012
- “A sieve strategy for irreducible tabulation;”  
invited talk at the UIUC Number Theory Seminar, April 2012
- “Algorithms for the subset-product problem;”  
invited talk at the ISU Discrete Math Seminar, February 2012
- “Constructing Carmichael numbers with many prime factors;”  
contributed talk at the West Coast Number Theory Conference, Pacific Grove, CA, December 2011
- “Constructing large numbers with cheap computers;”  
invited talk at the Wabash College math colloquium, October 2011
- “Constructing Carmichael numbers with a billion prime factors;”  
invited talk at the Brigham Young University number theory seminar, February 2011.
- “The fixed weight subset sum problem;”  
contributed talk at 24th Midwest Conference on Combinatorics, Cryptography, and Computing in Normal, IL, September 2010
- “Tabulating irreducible polynomials over finite fields;”  
contributed talk at Mathfest 2010 in Pittsburgh, August 2010

## TEACHING GOALS

---

To help students gain a deep understanding of mathematical concepts. To help students gain confidence in tackling difficult problems, mathematical or otherwise. To convince students that anyone can learn mathematics.

## TEACHING EXPERIENCE

---

- Assistant, Associate Professor at Illinois Wesleyan University, Fall 2009 – present
- Sessional instructor at University of Calgary, Fall 2007 – Spring 2009
- Teaching assistant at University of Wisconsin–Madison, Fall 2000 – Spring 2002, Fall 2004 – Spring 2006
- KTI fellow, Summer 2002 – Summer 2004 (Kindergarten Through Infinity, a National Science Foundation GK-12 fellowship); duties included working closely with high school math teachers to design and discuss 9th grade algebra curriculum and to help implement it in the classroom, also to participate in professional development seminars and workshops for Madison math teachers and KTI fellows

## COURSES TAUGHT AT ILLINOIS WESLEYAN

---

- Fall 2009: Math 161 (Calculus 1), Math 263 (Calculus 3), Math 105 (Math Concepts for Elementary Education 1)
- Spring 2010: Math 161 (Calculus 1), Math 162 (Calculus 2), Math 370 (Number Theory)
- Fall 2010: Math 161 (Calculus 1), Math 105 (Math Concepts for Elementary Education 1), Math 200 (Techniques of Proof)
- Spring 2011: Math 161 (Calculus 1), Math 162 (Calculus 2), Math 166 (Analysis 2)
- Fall 2011: Math 161 (Calculus 1), Math 165 (Analysis 1), Math 105 (Math Concepts for Elementary Education 1), Math 495 (Directed Study)
- Spring 2012: Math 106 (Math Concepts for Elementary Education 2), Math 166 (Analysis 2), Math 405 (Modern Algebra), Math 499 (Research/Thesis)
- Fall 2012: Math 165 (Analysis 1), Math/CS 136 (Computational Discrete Math), Math 337 (Algorithmic Number Theory)
- Spring 2013: Math 110 (Finite Mathematics), Math 166 (Analysis 2), Math/CS 135 (Application of Sets, Logic, and Recursion)
- Fall 2013: Math 161 (Calculus 1), Math 165 (Analysis 1), Math/CS 136 (Computational Discrete Math)
- Spring 2014: Math 166 (Analysis 2), Math 263 (Calculus 3), Math 405 (Modern Algebra)
- Fall 2014: Math 105 (Math Concepts for Elementary Education 1), Math 161 (Calculus 1), Math 165 (Analysis 1)
- Spring 2015: Math 106 (Math Concepts for Elementary Education 2), Math 161 (Calculus 1), Math 337 (Algorithmic Number Theory)
- Fall 2015: on sabbatical
- Spring 2016: Math 106 (Math Concepts for Elementary Education 2), Math 110 (Finite Math), Math 405 (Modern Algebra)

#### SELECTED PRESENTATIONS

---

- “Modular arithmetic and cryptography,” presentation to the Illinois Mathematics and Science Academy group at Bloomington Junior High School, May 2014.
- “Constructing large numbers with cheap computers,” keynote speech for the Kappa Mu Epsilon induction ceremony (a national mathematics honors society), Dominican University, April 2014.
- “Making faculty meetings productive,” joint presentation with Joerg Tiede on parliamentary procedure, Illinois Wesleyan University, January 2014.
- “How many primes?” keynote speech for 2014 Pi Mu Epsilon high school math contest.
- “Constructing large numbers with cheap computers,” Illinois State summer REU (Research Experience for Undergraduates) for future secondary math teachers, June 2013.
- “How your credit card is protected online,” IWU non-org talk, November 2010.
- “Cryptography and careers in computer security,” keynote speech for the 2010 Pi Mu Epsilon high school math contest.

#### SERVICE GOALS

---

To contribute to faculty governance at Illinois Wesleyan University, and to improve the education of future teachers of mathematics.

#### SERVICE TO THE MATHEMATICAL COMMUNITY

---

- Board member at large, board of directors for the Illinois Section of the Mathematical Association of America (ISMAA).
- Helped organize a panel entitled “Getting Discovery Learning Started,” for Project NExT fellows at the 2010 Joint Mathematics Meetings in San Francisco.
- Referee for five papers during the period August 2009 - July 2014. These papers were from mathematics, computer science, and cryptography.

#### SERVICE TO ILLINOIS WESLEYAN UNIVERSITY

---

- Assessment Committee member, starting Fall 2014.
- Formal Reasoning Assessment Liaison, tasked with organizing assessment of the formal reasoning category of the general education program, Spring 2014 - Fall 2015.
- Faculty Parliamentarian, Fall 2012 - present.
- Faculty Secretary, 2010-2011 and 2011-2012 school years.
- Member of Teacher Education Committee, 2009-present.
- Representative to the board of directors of the Great Lakes Consortium on Petascale Computing, 2010-2011 and 2011-2012 school years.
- Research honor committees: Amanda Clayton '10 (Economics), Taole Zhu '11 (Mathematics), Steven Hayman '12 (Mathematics), Jordyn Maglalang '12 (Computer Science), Nick Nichols '13 (Computer Science), Ammar Malik '13 (Computer Science), Tom Simmons '14 (Mathematics).

#### SERVICE TO THE MATHEMATICS DEPARTMENT

---

- Liaison to the Ed Studies Department, Fall 2009 - present.
- Faculty advisor for the local chapter of Pi Mu Epsilon, Fall 2012 - present.
- Coach for participants of the Putnam Mathematics Competition, Fall 2010 - present.
- Various routine jobs, including contributions to department meetings, crafting policy changes, advising, and sitting on search committees.

#### HONORS, AWARDS, MEMBERSHIPS

---

- Spring 2015: awarded ASD grant, which paid for a trip to Calgary during my sabbatical semester (Fall 2015) to work on Lucas pseudoprimes.
- Summer 2014: faculty advisor for Tom Simmons' award of an Eckley Fellowship, an internal grant that supports undergraduate summer research.
- December 2013: awarded an assignment grant to address information literacy in Math 405 (Modern Algebra). This was an internal award, part of a larger Mellon Grant administered by the Writing Program at IWU.

- Fall 2012: invited to give a Faculty Colloquium.
- December 2011: awarded ASD grant, the bulk of which went to pay a summer student to implement a program that proves primality of an integer  $n$  given the factorization of  $n + 1$ .
- Spring 2011: awarded ASD grant, the bulk of which went to pay a summer student to do programming work as part of a project to construct large Carmichael numbers.
- Fall 2009: awarded CD grant to develop a course related to number theory and cryptography. This has become Math 337, Algorithmic Number Theory.
- Project NExT fellow for 2009-2010 (New Experiences in Teaching, a program of the Mathematical Association of America for new faculty in mathematics).
- KTI fellow, Summer 2002 – Summer 2004 (Kindergarten Through Infinity, an NSF GK-12 fellowship).
- member of the Mathematical Association of America